PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-261788

(43)Date of publication of application : 13.09.2002

(51)Int.Cl. H04L 12/46
G06F 13/00
H04L 12/66

(21)Application number : 2001-052950

(22)Date of filing : 27.02.2001

(71)Applicant : MITSUBISHI ELECTRIC CORP

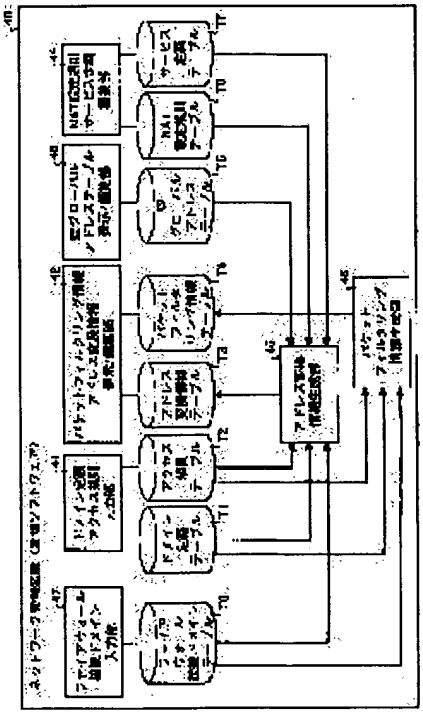
(72)Inventor : KANAEGAMI ATSUSHI

(54) FIREWALL MANAGING APPARATUS AND METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain a firewall managing apparatus and a method which can form batch setting information of firewall which includes not only packet filtering information but also address conversion information of an NAT by using definition description easy to be understood by a person, in order to mutually operate a plurality of bases via an internet.

SOLUTION: On the basis of a domain definition table T1 and an access rule table T2 as the operation policy of a LAN 12 and a LAN 13, a vacant global address table T5, an NAT-setting rule table T6 and a service definition table T7, NAT address conversion information D1b, D2b and packet filtering information D1a, D2a are formed by using firewalls FW1, FW2 of the LANs 12, 13.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or

application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－261788
（P2002－261788.A）
(43)公開日　平成14年９月13日(2002.9.13)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｌ　12/46		Ｈ０４Ｌ　12/46	Ｅ	５Ｂ０８９
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ	５Ｋ０３０
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　12/66	Ｂ	５Ｋ０３３

審査請求　未請求　請求項の数９　ＯＬ　（全 15 頁）

(21)出願番号　特願2001－52950(P2001－52950)

(22)出願日　平成13年２月27日(2001.2.27)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

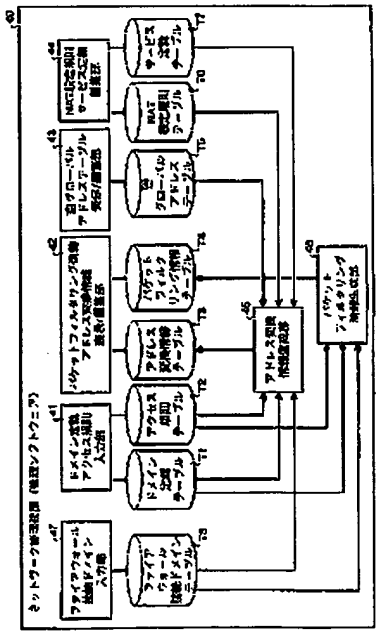
(72)発明者　金枝上　敬史
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

(74)代理人　100089118
弁理士　酒井　宏明

Ｆターム(参考)　5B089 DA06 KA17 KB04 KB13
5K030 GA15 HA08 HB08 HC01 HC14 HD06 JL07
5K033 AA08 CB09 DA06 DB18 DB20 EA07 EC03

(54)【発明の名称】　ファイアウォール管理装置および方法

(57)【要約】
【課題】　インターネットを介して複数拠点間を相互運用するため、人間に判りやすい定義記述を用いてパケットフィルタリング情報だけでなくＮＡＴのアドレス変換情報を含めたファイアウォールの設定情報を一括生成し得るファイアウォール管理装置および方法を得ること。
【解決手段】　各ＬＡＮ１２，１３の適用ポリシーとしてのドメイン定義テーブルＴ１，アクセス規則テーブルＴ２と、空グローバルアドレステーブルＴ５と、ＮＡＴ設定規則テーブルＴ６と、サービス定義テーブルＴ７とに基づいて各ＬＡＮ１２、１３のファイアウォールＦＷ１，ＦＷ２で用いてＮＡＴアドレス変換情報Ｄ１ｂ，Ｄ２ｂおよびパケットフィルタリング情報Ｄ１ａ，Ｄ２ａを生成する。



1

【特許請求の範囲】

【請求項１】　ＮＡＴ機能を持つファイアウォール、１～複数の端末および１～複数のサーバを夫々有する複数のＬＡＮ間がインターネットを介して接続されるネットワークに適用され、前記各ＬＡＮのファイアウォールの設定情報を管理するファイアウォール管理装置において、

前記複数のＬＡＮの運用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレス、ＮＡＴ設定規則、サービス定義に関する情報が予め登録されるデータベースと、

このデータベースに蓄積された情報に基づいて前記複数のＬＡＮの各ファイアウォールのＮＡＴアドレス変換情報を作成するアドレス変換情報作成手段と、

前記データベースに蓄積された情報に基づいて前記複数のＬＡＮの各ファイアウォールのパケットフィルタリング情報を作成するパケットフィルタリング作成手段と、

を備えることを特徴とするファイアウォール管理装置。

【請求項２】　前記各ＬＡＮに含まれる端末およびサーバを、端末とサーバとを別グループとして複数のグループに分け、該分けたグループ間でのアクセス規則を前記運用ポリシーとして前記データベースに蓄積すること特徴とする請求項１に記載のファイアウォール管理装置。

【請求項３】　前記アクセス規則は、当該ＬＡＮの１つの端末グループから他のＬＡＮの１つのサーバグループへのアクセスをアクセス規則の単位として、管理すべき複数のＬＡＮ内に含まれる全ての端末グループおよびサーバグループについて登録されることを特徴とする請求項２に記載のファイアウォール管理装置。

【請求項４】　前記アクセス規則には、前記分けられたグループ毎にグローバルアドレスの割当数が設定されることを特徴とする請求項２または３に記載のファイアウォール管理装置。

【請求項５】　前記アクセス規則には、各アクセス規則毎に、プロトコル種別、サービス種別、同じグループ内での各端末の同時接続の有無が登録されることを特徴とする請求項３または４に記載のファイアウォール管理装置。

【請求項６】　前記ＮＡＴ設定規則には、端末およびサーバの区別、自グループ内の端末またはサーバの同時接続の有無、サービス指定ポート番号の有無が登録され、ＮＡＴ設定規則はこれら３つの登録情報に基づいてＮＡＴ種別を分類することを特徴とする請求項２～５のいずれか一つに記載のファイアウォール管理装置。

【請求項７】　前記サービス定義には、サービス種別、端末およびサーバの区別、指定ポート番号が登録されていることを特徴とする請求項２～６のいずれか一つに記載のファイアウォール管理装置。

【請求項８】　前記運用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレス、ＮＡＴ設定規則、サービス定義に関する情報を編集し、該編集結果を前記データベースに登録する手段を備えることを特徴とする請求項１～７のいずれか一つに記載のファイアウォール管理装置。

2

【請求項９】　ＮＡＴ機能を持つファイアウォール、１～複数の端末および１～複数のサーバを夫々有する複数のＬＡＮ間がインターネットを介して接続されるネットワークに適用され、前記各ＬＡＮのファイアウォールの設定情報を管理するファイアウォール管理方法において、

前記複数のＬＡＮの運用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレス、ＮＡＴ設定規則、サービス定義に関する情報を予め登録するステップと、

このデータベースに蓄積された情報に基づいて前記複数のＬＡＮの各ファイアウォールのＮＡＴアドレス変換情報およびパケットフィルタリング情報を作成するステップと、

を備えることを特徴とするファイアウォール管理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＮＡＴ機能を持つファイアウォールの設定情報を自動作成するための技術に関し、特にインターネットを介した複数のＬＡＮ（ローカルエリアネットワーク）間を接続するための運用ポリシーなどに基づいて各ＬＡＮにおけるファイアウォールのアドレス変換情報およびパケットフィルタリング情報を作成するファイアウォール管理装置および方法に関するものである。

【０００２】

【従来の技術】運用ポリシーからファイアウォールの設定情報を生成する技術は、ポリシーネットワーキングとして近年注目を集めている。

【０００３】従来、ファイアウォールの管理のためには、多数の運用ポリシーの管理が必要であり、そのためにはネットワークの高度な技術やベンダ固有の設定情報の習得を必要とする。また、ファイアウォールへの設定情報から第三者が網の運用ポリシーを理解するのは困難であった。

【０００４】そこで、ファイアウォールの運用ポリシーを管理する技術として、特開2000-253066号公報の「ファイアウォールを管理するための方法および装置」がある。この従来技術では、イントラネットのトポロジーとファイアウォールの運用規則の関係を表わすエンティティ関係モデルと、運用規則のインスタンスを定義するモデル定義言語とから、ファイルウォールに設定するコンフィグレーションファイルの生成を実現している。この技術によれば、運用規則とトポロジーを独立に管理することができ、トポロジーが変更されても運用規則を書き換える必要がなく、運用ポリシーの再利用が可能とな

る。この従来技術では、生成される設定情報は、パケットフィルタリングとフィルタリングの優先度に関するものしかない。

【０００５】また、特開2000-244495号公報の「ネットワーク管理システム」には、独立性を保って定義した運用規則と網トポロジーとからファイアウォールやルータの設定情報を生成することが開示されており、ファイアウォールの規則の複雑さ、規則の順番、他の設定情報との整合性を意識せずに管理者がセキュリティポリシーを設計できるようにしている。また、セキュリーティポリシーを装置固有の設定情報のシンクタスおよびセマンテクスから分離することにより、ポリシー定義情報の共有および再利用を可能とすることが示されている。

【０００６】

【発明が解決しようとする課題】しかしながら、これらの従来技術には、ＬＡＮ内での運用ポリシーを管理することしか開示されておらず、インターネットを介した複数のＬＡＮ間での運用ポリシーを統括して管理することは何ら開示されていない。このようなインターネットを介した複数のＬＡＮ間での運用ポリシーの管理に対する要求は、専用線を持たずに離れた複数の拠点間をインターネットを介して相互運用したい状況下で発生する。

【０００７】近年、ＩＰアドレスの枯渇を解決するために、スタブドメインの境界にＮＡＴ（Network Address Translation ネットワークアドレス変換）を置くことが提案されている。ＮＡＴは、ＬＡＮ内だけで用いられるローカルアドレス（プライベートアドレス）とインターネットで用いられるグローバルにユニークなグローバルアドレスとの間でアドレス変換する技術である。そして、ファイアウォールにもＮＡＴ機能を付加機能として設けることが提案されている。

【０００８】ＮＡＴを用いて複数のＬＡＮ間を接続するための管理装置を提供するためには、上記従来技術のようなパケットフィルタリング情報だけでなく、ＮＡＴで用いられるローカルアドレスとグローバルアドレスのアドレス変換情報をファイアウォールに設定する必要がある。

【０００９】しかしながら、前述したように、上記従来技術では、ＬＡＮ内での運用ポリシーを管理するべく主にパケットフィルタリング情報を生成することしか開示されておらず、インターネットを介した複数のＬＡＮ間で運用ポリシーを管理するためにパケットフィルタリング情報のみならずＮＡＴのアドレス変換情報を生成することは開示されてはいない。

【００１０】この発明は上記に鑑みてなされたもので、インターネットを介して複数拠点間を相互運用するため、人間に判りやすい定義記述を用いてパケットフィルタリング情報だけでなくＮＡＴのアドレス変換情報を含めたファイアウォールの設定情報を生成することができるファイアウォール管理装置および方法を得ることを目的としている。

【００１１】

【課題を解決するための手段】上記目的を達成するためこの発明では、ＮＡＴ機能を持つファイアウォール、１～複数の端末および１～複数のサーバを夫々有する複数のＬＡＮ間がインターネットを介して接続されるネットワークに適用され、前記各ＬＡＮのファイアウォールの設定情報を管理するファイアウォール管理装置において、前記複数のＬＡＮの運用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレス、ＮＡＴ設定規則、サービス定義に関する情報が予め登録されるデータベースと、このデータベースに蓄積された情報に基づいて前記複数のＬＡＮの各ファイアウォールのＮＡＴアドレス変換情報を作成するアドレス変換情報作成手段と、前記データベースに蓄積された情報に基づいて前記複数のＬＡＮの各ファイアウォールのパケットフィルタリング情報を作成するパケットフィルタリング作成手段とを備えることを特徴とする。

【００１２】この発明によれば、複数のＬＡＮの運用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレス、ＮＡＴ設定規則、サービス定義に関する情報を用いてＮＡＴアドレス変換情報およびパケットフィルタリング情報を生成するようにしたので、ＮＡＴを用いて複数のＬＡＮ間を接続するための各ファイアウォールでの所要の設定情報を一括して簡単に作成することができる。

【００１３】つぎの発明によれば、上記発明において、前記各ＬＡＮに含まれる端末およびサーバを、端末とサーバとを別グループとして複数のグループに分け、該分けたグループ間でのアクセス規則を前記運用ポリシーとして前記データベースに蓄積すること特徴とする。

【００１４】この発明によれば、端末とサーバとを別グループとして複数のグループに分け、該分けたグループ間でのアクセス規則を前記運用ポリシーとして前記データベースに蓄積している。

【００１５】つぎの発明によれば、前記アクセス規則は、当該ＬＡＮの１つの端末グループから他のＬＡＮの１つのサーバグループへのアクセスをアクセス規則の単位として、管理すべき複数のＬＡＮ内に含まれる全ての端末グループおよびサーバグループについて登録されることを特徴とする。

【００１６】この発明によれば、当該ＬＡＮの１つの端末グループから他のＬＡＮの１つのサーバグループへのアクセスを単位として、アクセス規則を登録している。

【００１７】つぎの発明によれば、上記発明において、前記アクセス規則には、前記分けられたグループ毎にグローバルアドレスの割当数が設定されることを特徴とする。

【００１８】この発明によれば、アクセス規則にグローバルアドレスの割当数がグループ毎に設定している。

【００１９】つぎの発明によれば、上記発明において、前記アクセス規則には、各アクセス規則毎に、プロトコル種別、サービス種別、同じグループ内での各端末の同時接続の有無が登録されることを特徴とする。

【００２０】この発明によれば、アクセス規則には、プロトコル種別、サービス種別、同じグループ内での各端末の同時接続の有無が登録されている。

【００２１】つぎの発明によれば、上記発明において、ＮＡＴ設定規則には、端末およびサーバの区別、自グループ内の端末またはサーバの同時接続の有無、サービス指定ポート番号の有無が登録され、ＮＡＴ設定規則はこれら３つの登録情報に基づいてＮＡＴ種別を分類することを特徴とする。

【００２２】この発明によれば、端末およびサーバの区別、自グループ内の端末またはサーバの同時接続の有無、サービス指定ポート番号の有無に基づいてＮＡＴ種別が分類される。

【００２３】つぎの発明によれば、上記発明において、前記サービス定義には、サービス種別、端末およびサーバの区別、指定ポート番号が登録されていることを特徴とする。

【００２４】この発明によれば、前記サービス定義には、サービス種別、端末およびサーバの区別、指定ポート番号が登録されている。

【００２５】つぎの発明によれば、上記発明において、前記適用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレス、ＮＡＴ設定規則、サービス定義に関する情報を編集し、該編集結果を前記データベースに登録する手段を備えることを特徴とする。

【００２６】この発明によれば、上記の各種情報を編集し、該編集結果を前記データベースに登録する手段を備えているので、適用ポリシー、ＬＡＮの構成などが変更された場合にもこれに容易に対処することができる。

【００２７】つぎの発明によれば、ＮＡＴ機能を持つファイアウォール、１～複数の端末および１～複数のサーバを夫々有する複数のＬＡＮ間がインターネットを介して接続されるネットワークに適用され、前記各ＬＡＮのファイアウォールの設定情報を管理するファイアウォール管理方法において、前記複数のＬＡＮの適用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレス、ＮＡＴ設定規則、サービス定義に関する情報を予め登録するステップと、このデータベースに蓄積された情報に基づいて前記複数のＬＡＮの各ファイアウォールのＮＡＴアドレス変換情報およびパケットフィルタリング情報を作成するステップとを備えることを特徴とする。

【００２８】この方法発明によれば、複数のＬＡＮの適用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレス、ＮＡＴ設定規則、サービス定義に関する情報を用いてＮＡＴアドレス変換情報およびパケットフィルタリング情報を生成するようにしたので、ＮＡＴを用いて複数のＬＡＮ間を接続するための各ファイアウォールでの所要の設定情報を一括して簡単に作成することができる。

【００２９】

【発明の実施の形態】以下に添付図面を参照して、この発明にかかるファイアウォール管理装置および方法の好適な実施の形態を詳細に説明する。

【００３０】実施の形態１．初めに、本発明の対象とするネットワーク構成の一例を説明する。図１はＮＡＴ機能とパケットフィルタリング機能を持つファイアウォールＦＷ１およびＦＷ２を用い、インターネット１１を介して２つのＬＡＮ１２，１３を接続した網構成を示すものである。

【００３１】ファイアウォールＦＷ１（ファイアウォール１）の内部でローカルエリアネットワークを構成するＬＡＮ１２およびファイアウォールＦＷ２（ファイアウォール２）の内部でローカルエリアネットワークを構成するＬＡＮ１３は、例えば、夫々、同じ会社の距離の離れた工場で構成されたネットワークである。ＬＡＮ接続された各工場は、協力して製品開発をおこなっており、それぞれの工場の設計担当者は端末パソコンを用いて設計作業をおこない、工場間の設計者間では、インターネット１１を介して設計データの交換を可能としているものとする。

【００３２】ＬＡＮ１２，１３は、ＩＰアドレスをローカルアドレス（プライベートアドレス）で管理しており、インターネット１１はＩＰアドレスを勿論グローバルアドレスで管理している。

【００３３】ファイアウォールＦＷ１は、ＬＡＮ１２内とインターネット１１との間でどのパケットを通過させるか否かを所定の規則に従って判定するパケットフィルタリング機能を有するとともに、インターネット１１からＬＡＮ１２内のローカルアドレスを隠蔽するため、パケット内のＩＰアドレスを変換するＮＡＴ機能を有している。ファイアウォールＦＷ１においては、後述するネットワーク管理装置の管理ソフトウェア４０によって作成されたパケットフィルタリング情報Ｄ１ａおよびアドレス変換情報Ｄ１ｂが蓄積記憶されており、これらの情報Ｄ１ａおよびＤ１ｂに基づいてパケットフィルタリング機能およびＮＡＴ機能を実行する。ファイアウォールＦＷ２も同様であり、後述するネットワーク管理装置の管理ソフトウェア４０によって作成されたパケットフィルタリング情報Ｄ２ａおよびアドレス変換情報Ｄ２ｂが蓄積記憶されており、これらの情報Ｄ２ａおよびＤ２ｂに基づいてパケットフィルタリング機能およびＮＡＴ機能を実行する。

【００３４】この場合、ＬＡＮ１２内には、２つのクライアント端末（以下単に端末という）２１，２２と２つ

のサーバ２３，２４とが含まれている。クライアント端末２１，２２は１つの端末ドメイン１４（端末ドメインＡともいう）に属し、サーバ２３，２４は、１つのサーバドメイン１５（サーバドメインＢともいう）に属している。この場合は、便宜上１つの端末ドメインＡおよびサーバドメインＡしか示していないが、通常は１～複数の端末ドメインおよびサーバドメインが含まれる。

【００３５】ＬＡＮ１３内には、この場合、２つのクライアント端末３１，３２と２つのサーバ３３，３４とが含まれている。クライアント端末３１，３２は１つの端末ドメイン１６（端末ドメインＢともいう）に属し、サーバ３３，３４は、１つのサーバドメイン１７（サーバドメインＢともいう）に属している。ＬＡＮ１３にも、通常は、１～複数の端末ドメインおよびサーバドメインが含まれる。

【００３６】通常、各ＬＡＮ１２，１３には、複数のホスト（端末およびサーバ）が含まれているが、これら複数のホストを端末とサーバとを別グループとして、任意の複数のグループに分け、これら分けた１つのグループを本明細書中ではドメインと呼称している。したがって、分割された１つのグループに１つのドメイン名が割り振られる。上記グループ（ドメイン）の単位は、例えば、工場内の経理グループ、総務グループ、技術グループなどであり、業務種別によって分けたグループ毎に所定のドメイン名が割り振られる。したがって、この場合、ＬＡＮ１２には、ドメイン名が端末ドメインＡである端末ドメイン１４とドメイン名がサーバドメインＡであるサーバドメイン１５との２つのグループ（ドメイン）が存在し、ＬＡＮ１３には、ドメイン名が端末ドメインＢである端末ドメイン１６とドメイン名がサーバドメインＢであるサーバドメイン１７との２つのグループ（ドメイン）が存在している。

【００３７】ＬＡＮ１２内の各ホスト（端末２１，２２およびサーバ２３，２４）には、図１に示すように、当該ＬＡＮ内で一意なローカルＩＰアドレスＬ１～Ｌ４がそれぞれ割り振られており、また、ＬＡＮ１３内の各ホスト（端末３１，３２およびサーバ３３，３４）には、当該ＬＡＮ内で一意なローカルＩＰアドレスＬ１０１～Ｌ１０４が夫々割り振られている。

【００３８】この図１の網構成では、以下の３種類のＮＡＴ機能を持つものとする。

【００３９】Basic NAT

ＩＰアドレスを対象としたアドレス変換方式であり、割当ＩＰアドレスとして、アドレス変換規則に指定された割当ＩＰアドレス範囲のなかの空きＩＰアドレスが動的に割り当てられる。同一ローカルＩＰアドレスを端点とする通信フローは同一の割当ＩＰアドレスを共有する。

【００４０】Static NAT

グローバルＩＰアドレスとローカルＩＰアドレスの変換の組合せをスタティックに決める。サーバのようにグローバルアドレスを固定しなくてはならないときに用いる。

【００４１】NAPT

ＩＰアドレスおよびＴＣＰ（ＵＤＰ）ポート番号を変換対象としたアドレス変換方式であり、ローカルＩＰアドレスとグローバルＩＰアドレスとの間で多対１の変換を可能にする方式がある。このNAPT方式は、同じグローバルアドレスの複数ポート番号にローカルＩＰアドレスを割り当てる。

【００４２】図２はファイアウォールＦＷ１，ＦＷ２への設定情報を生成するネットワーク管理装置（ファイアウォール管理装置）に内蔵される管理ソフトウェア４０の機能構成の一例を示したものである。

【００４３】図２において、ドメイン定義アクセス規則入力部４１、パケットフィルタリング情報アドレス変換情報表示／編集部４２、空グローバルアドレステーブル表示／編集部４３、ＮＡＴ設定規則サービス定義編集部４４、ファイアウォール接続ドメイン入力部４７は、管理者と各テーブルＴ１～Ｔ８とのインタフェースである。

【００４４】ドメイン定義テーブルＴ１，アクセス規則テーブルＴ２，アドレス変換情報テーブルＴ３，パケットフィルタリング情報テーブルＴ４，空グローバルアドレステーブルＴ５，ＮＡＴ設定規則テーブルＴ６，サービス定義テーブルＴ７およびファイアウォール接続ドメインテーブルＴ８は、各種テーブルを格納するデータベースである。

【００４５】アドレス変換情報生成部４５およびパケットフィルタリング情報生成部４６は、ファイアウォールＦＷ１およびＦＷ２の設定情報（アドレス変換情報およびパケットフィルタリング情報）を生成するプログラムである。

【００４６】以下、個々の詳細について説明する。ドメイン定義アクセス規則入力部４１は、ドメイン定義テーブルＴ１およびアクセス規則テーブルＴ２に対し、ドメイン定義およびアクセス規則を入出力するための管理者とのインタフェースである。管理者は、このドメイン定義アクセス規則入力部４１を介して当該網構成すなわちインターネット１１を介して接続されるＬＡＮ１１，１２の運用ポリシーを定義する。

【００４７】パケットフィルタリング情報アドレス変換情報表示／編集部４２は、作成されたアドレス変換情報テーブルＴ３のアドレス変換情報およびパケットフィルタリング情報テーブルＴ４のパケットフィルタリング情報を表示および編集するためのユーザインタフェースであり、編集の結果は再びアドレス変換情報テーブルＴ３およびパケットフィルタリング情報テーブルＴ４に格納される。

【００４８】空グローバルアドレステーブル表示／編集部４３は、各ＬＡＮ１２，１３に割当て可能な空グロー

バルアドレスを管理するためのユーザインタフェースであり、空グローバルアドレスの表示、追加、削除を行う。空グローバルアドレスの編集結果は、空グローバルアドレステーブルＴ５に登録される。

【００４９】ＮＡＴ設定規則サービス定義編集部４４は、ＮＡＴ設定規則およびサービス定義情報を表示編集するためのインタフェースであり、それらの編集結果をＮＡＴ設定規則テーブルＴ６、サービス定義テーブルＴ７に蓄積する。

【００５０】ファイアウォール接続ドメイン入力部４７は、各ファイアウォールＦＷ１，ＦＷ２に接続される接続ドメインをファイアウォール接続ドメインテーブルＴ８に登録、編集するためのインタフェースである。

【００５１】ファイアウォール接続ドメインテーブルＴ８には、図３に示すように、各ファイアウォールＦＷ１，ＦＷ２に接続される接続ドメインがファイアウォールＦＷ１，ＦＷ２毎に登録される。この場合、図１に示すように、ファイアウォールＦＷ１には、端末ドメインＡおよびサーバドメインＡが接続され、またファイアウォールＦＷ２には、端末ドメインＢおよびサーバドメインＢが接続される。

【００５２】ドメイン定義テーブルＴ１には、図４に示すように、インターネット１１を介した２つのＬＡＮ１２および１３のドメイン定義が蓄積記憶される。このドメイン定義には、ドメイン（ドメイン名、グループ）毎に、ドメイン種別（端末かサーバかの区別）と、当該ドメインに割り振られたホストアドレス（ローカルＩＰアドレス）とが登録される。このドメイン定義は、図５に示すアクセス規則（アクセス定義）と共に、管理者が、各ＬＡＮ１２，１３で用いる運用ポリシーとして、予め定義する。例えば、ドメイン名が端末ドメインＡである場合は、ドメイン種別は端末であり、このドメインＡには、ローカルＩＰアドレスがＬ１，Ｌ２である２つの端末が含まれることになる。

【００５３】アクセス規則テーブルＴ２には、図５に示すように、インターネット１１を介した２つのＬＡＮ１２および１３のアクセス規則が記憶される。このアクセス規則は、図４に示したドメイン定義と共に、管理者が、各ＬＡＮ１２，１３で用いる運用ポリシーとして、予め定義する。アクセス規則は、必要な複数のアクセス規則から成る。すなわち、アクセス規則は、当該ＬＡＮの１つの端末ドメインから他のＬＡＮの１つのサーバドメインへのアクセスをアクセス規則の単位（１つの規則名）として、管理すべき複数のＬＡＮ内に含まれる全ての端末グループおよびサーバグループについて登録される。各アクセス規則には、規則名（この場合、ＰＪ１－１，ＰＪ１－２の２つの規則名）、適用ドメインfrom（端末側ドメイン）、適用ドメインto（サーバ側ドメイン）、用いるプロトコル種別（この場合はＴＣＰ）、可能なサービス種別（この場合はＦＴＰ）、ドメイン内での複数の同時接続の有無、が含まれている。適用ドメインfromには、ドメイン名と割当アドレス数（割当可能なグローバルＩＰアドレス数）が含まれている。適用ドメインtoには、ドメイン名、割当アドレス数（割当可能なグローバルＩＰアドレス数）が含まれている。この場合は、端末ドメインＡおよびＢの割当アドレス数は夫々１である。サーバドメインには、当該サーバドメインに含まれるサーバ数分のグローバルＩＰアドレスが必要なので、サーバドメインの割当アドレス数はこのテーブルＴ２では登録されていない。

【００５４】空グローバルアドレステーブルＴ５には、図６に示すように、各ファイアウォールＦＷ１，ＦＷ２毎に割当可能な空グローバルＩＰアドレスが記憶される。この場合、ファイアウォールＦＷ１には、複数のグローバルＩＰアドレスＧ１，Ｇ２，…が割り振られ、ファイアウォールＦＷ２には、複数のグローバルＩＰアドレスＧ１０１，Ｇ１０２，…が割り振られている。このテーブルＴ５も、管理者が予め作成登録する。

【００５５】ＮＡＴ設定規則テーブルＴ６は、図７に示すように、上記した３つのＮＡＴ種別のうちの１つを選択するための規則が設定されたテーブルである。このテーブルＴ６も、管理者が予め作成登録するものであり、この登録内容に応じてアドレス変換情報生成部４５での後述する処理手順（アルゴリズム）が決定される。図７の場合は、ドメイン種別が端末で、自ドメイン内での複数同時接続がありで、サービス指定ポート番号がある場合、あるいは、ドメイン種別が端末で、自ドメイン内での複数同時接続がなしで、サービス指定ポート番号がある場合は、Basic NATが選択される。ドメイン種別が端末で、自ドメイン内での複数同時接続がありで、サービス指定ポート番号がない場合、あるいは、ドメイン種別が端末で、自ドメイン内での複数同時接続がなしで、サービス指定ポート番号がない場合は、NAPTが選択される。ドメイン種別がサーバである場合は、Static NATが選択される。

【００５６】サービス定義テーブルＴ７には、図８に示すように、サービス種別（この場合はＦＴＰのみ）および指定ポート番号の有無ならびに指定ポート番号の内容が設定される。この場合は、ＦＴＰの場合は、ドメイン種別が端末のときは、ポート番号の指定はなしとし、ドメイン種別がサーバのときは、２つのポート番号が設定されるようにしている。このテーブルＴ７も、管理者が予め作成登録する。

【００５７】アドレス変換情報生成部４５は、ＮＡＴアドレス変換情報の生成手順が実装されたプログラムであり、ドメイン定義テーブルＴ１に記憶されたドメイン定義、アクセス規則テーブルＴ２に記憶されたアクセス規則、空グローバルアドレステーブルＴ５に記憶内容、ＮＡＴ設定規則テーブルＴ６に記憶されたＮＡＴ設定規則、サービス定義テーブルＴ７に記憶されたサービス定

義に基づいてファイアウォールＦＷ１およびＦＷ２のＮＡＴアドレス変換情報を作成し、該作成したアドレス変換情報をアドレス変換情報テーブルＴ３に記憶する。

【００５８】アドレス変換情報テーブルＴ３には、図１０および図１１に示すような、アドレス変換情報生成部４５によって作成されたファイアウォールＦＷ１およびＦＷ２のＮＡＴアドレス変換情報が記憶される。このアドレス変換情報テーブルＴ３の記憶内容は、パケットフィルタリング情報アドレス変換情報表示／編集部４２を介して管理者が適宜編集することができる。

【００５９】パケットフィルタリング情報生成部４６は、ファイアウォールＦＷ１およびＦＷ２のパケットフィルタリング情報の生成手順が実装されたプログラムであり、ドメイン定義テーブルＴ１に記憶されたドメイン定義、アクセス規則テーブルＴ２に記憶されたアクセス規則に基づいてファイアウォールＦＷ１およびＦＷ２のパケットフィルタリング情報を作成し、該作成したパケットフィルタリング情報をパケットフィルタリング情報テーブルＴ４に記憶する。

【００６０】パケットフィルタリング情報テーブルＴ４には、図１５、図１６に示すように、パケットフィルタリング情報生成部４６によって作成されたファイアウォールＦＷ１およびＦＷ２のパケットフィルタリング情報が記憶される。このパケットフィルタリング情報テーブルＴ４の記憶内容は、パケットフィルタリング情報アドレス変換情報表示／編集部４２を介して管理者が適宜編集することができる。

【００６１】図９は、アドレス変換情報生成部４５によって行なわれるＮＡＴアドレス変換情報の作成手順を示すものである。以下、この作成手順の詳細を説明する。

【００６２】図９の手順の前に、アドレス変換情報生成部４５は、図３に示すファイアウォール接続ドメインテーブルＴ８の登録内容を読み出すことにより、今回のアドレス変換情報作成処理を行うファイアウォール（この場合は２つのファイアウォールＦＷ１およびＦＷ２）と、これらファイアウォールに接続されるドメインに関する登録内容を認知している。

【００６３】まず、図５に示すアクセス規則テーブルＴ２の登録アクセス規則から１つのアクセス規則（例えば規則名ＰＪ１－１）を取り出し（ステップＳ１０１）、さらに取り出したアクセス規則からこのアクセス規則に属する適用ドメインfromあるいは適用ドメインtoを取り出す（ステップＳ１０２）。そして、図４に示すドメイン定義テーブルＴ１の内容も参照することにより、取り出した適用ドメインfrom（あるいはto）のドメイン名（例えば端末ドメインＡ）に対応するドメイン種別が端末であるかサーバであるかを判定する（ステップＳ１０３）。

【００６４】ステップＳ１０３の判定の結果がサーバである場合は、ＮＡＴ種別をStatic NATとする（ステップＳ１０８）。このＮＡＴ種別の選択は、図７に示したＮＡＴ設定規則テーブルＴ６の登録内容に基づいて行われている。

【００６５】ステップＳ１０３の判定の結果が端末である場合は、つぎに、取り出したアクセス規則における複数同時接続の有無の欄（図５参照）を参照することにより、ドメイン内での同時接続があるか否かを判定する（ステップＳ１０４）。この判定の結果、同時接続が行われない場合は、ＮＡＴ種別をBasic NATとする（ステップＳ１０９）。

【００６６】ステップＳ１０４で同時接続があると判定された場合は、つぎに、取り出したアクセス規則の適用ドメインfrom（あるいはto）の割当アドレス数の欄（図５参照）を参照することにより、当該ドメインに複数のグローバルアドレスを割り当てているか否かを判定する（ステップＳ１０５）。当該ドメインに複数のグローバルアドレスを割り当てていると判定された場合は、ＮＡＴ種別をBasic NATとする（ステップＳ１０９）。

【００６７】ステップＳ１０５で、当該ドメインに複数のグローバルアドレスを割り当てていないと判定された場合は、つぎに、図８に示したサービス定義テーブルＴ７の登録内容も参照して、利用されるサービス種別（この実施例ではＦＴＰ）にポート番号指定があるか否かを判定する（ステップＳ１０６）。

【００６８】ステップＳ１０６でポート番号指定があると判定された場合は、ＮＡＴ種別をBasic NATとする（ステップＳ１０９）。また、ステップＳ１０６でポート番号指定がないと判定された場合は、ＮＡＴ種別をNAPTとする（ステップＳ１０７）。

【００６９】上述のような処理によって、手順がステップＳ１０７に移行されて、ＮＡＴ種別としてNAPTが選択された場合は、図６に示した空グローバルアドレステーブルＴ５から１個のグローバルアドレスを取り出し、該取り出した１個のグローバルアドレスをテーブルＴ５から削除する（ステップＳ１１０）。この場合、端末ドメインＢの場合は、NAPTが選択されることになるので、端末ドメインＢには１つのグローバルアドレスが割当てられることになる。

【００７０】また、手順がステップＳ１０９に移行されて、ＮＡＴ種別としてBasic NATが選択された場合は、当該読み出されたアクセス規則の適用ドメインfrom（あるいはto）の当該ドメイン名に対応する割当アドレス数を参照することにより、図６に示した空グローバルアドレステーブルＴ５から前記割当アドレス数分のグローバルアドレスを先頭から順に取り出し、該取り出した１～複数のグローバルアドレスをテーブルＴ５から削除する（ステップＳ１１１）。この場合、端末ドメインＡの場合は、Basic NATが選択されるが、図５のアクセス規則テーブルＴ２によれば、端末ドメインＡの割当アドレス数は１であるので、１個のグローバルアドレスが空グロ

ーバルアドレステーブルＴ５から取り出される。

【００７１】また、手順がステップＳ１０８に移行されて、ＮＡＴ種別としてStatic NATが選択された場合は、図５のアクセス規則テーブルＴ２および図４のドメイン定義テーブルＴ１を参照することにより、図６に示した空グローバルアドレステーブルＴ５から当該ドメイン（この場合はサーバ端末）のホスト数（サーバ数）分のグローバルアドレスを先頭から順に取り出し、該取り出した１～複数のグローバルアドレスをテーブルＴ５から削除する（ステップＳ１１２）。この場合、サーバドメインＡの場合は（サーバドメインＢも）、Static NATが選択されるが、図４のドメイン定義テーブルＴ１によれば、サーバドメインＡのホスト数は２であるので、２個のグローバルアドレスが空グローバルアドレステーブルＴ５から取り出される。

【００７２】このようなグローバルアドレスの取り出しの際、上記の場合は、グローバルアドレスを空グローバルアドレステーブルＴ５から早い者順に先頭から取り出すようにしているが、グローバルアドレスの割り当てのための所定の規則を作り、指定されたグローバルアドレスが既に割り当てられているか否かを管理するデータベースを作成してもよい。

【００７３】ステップＳ１０７～Ｓ１０９の何れかの手順が終了すると、取り出した適用ドメインに属するホストアドレス（ローカルアドレス）を図４に示したドメイン定義テーブルＴ１から取り出し、この取り出されたホストアドレス（ローカルアドレス）を先の手順で取り出されたグローバルアドレスおよびＮＡＴ種別に対応付けて、ローカルアドレス（ポート番号も用いる場合はポート番号も付加する）、グローバルアドレスおよびＮＡＴ種別を項目として含む図１０および図１１に示すようなアドレス変換情報を作成し、該作成したアドレス変換情報をアドレス変換情報テーブルＴ３に記憶する（ステップＳ１１３）。

【００７４】つぎに、同じアクセス規則に他の適用ドメインがあるか否かを判定する（ステップＳ１１４）。すなわち、先の手順で適用ドメインfromが選択されていたときには、この段階で、他方の適用ドメインtoが選択されることになる。そして、選択された適用ドメインに対し、前述したステップＳ１０３～ステップＳ１１３の手順が実行されることにより、当該適用ドメインに対応するアドレス変換情報が作成され、作成されたアドレス変換情報はアドレス変換情報テーブルＴ３に記憶される。

【００７５】当該アクセス規則に属する２つの適用ドメイン（適用ドメインfromおよび適用ドメインto）に関するアドレス変換情報作成処理が終了すると、ステップＳ１１４の判断はＮＯになり、手順はステップＳ１１５に移行される。

【００７６】ステップＳ１１５においては、図５に示すアクセス規則テーブルＴ２につぎのアクセス規則がある か否かが判定される。次のアクセス規則がある場合は、このアクセス規則に含まれる２つの適用ドメインについて、１つずつ、前述したステップＳ１０３～ステップＳ１１３の手順が実行されることにより、当該アクセス規則に含まれる２つの適用ドメインについてのアドレス変換情報が作成され、作成された各アドレス変換情報は前記同様にしてアドレス変換情報テーブルＴ３に記憶される。

【００７７】図５のアクセス規則テーブルＴ２に登録された全てのアクセス規則について、前述した処理を繰り返すことにより、図１０および図１１に示すような、各ＬＡＮ１２，１３のファイアウォールＦＷ１，ＦＷ２のアドレス変換情報が作成される。そして、このようなアドレス変換情報の作成によって、図３のドメイン定義テーブルＴ１に、図１２に示すように、グローバルアドレスが付加されたものが追加される。

【００７８】図１０は、ファイアウォールＦＷ１のアドレス変換情報ある。ローカルアドレスＬ１，Ｌ２は、グローバルアドレスＧ１にBasic NATによってアドレス変換される。ローカルアドレスＬ３は、グローバルアドレスＧ３にStatic NATによってアドレス変換される。ローカルアドレスＬ４は、グローバルアドレスＧ４にStatic NATによってアドレス変換される。

【００７９】図１１は、ファイアウォールＦＷ２のアドレス変換情報ある。ローカルアドレスＬ１０１，Ｌ１０２は、グローバルアドレスＧ１０１にNAPTによってアドレス変換される。ローカルアドレスＬ１０３は、グローバルアドレスＧ１０３にStatic NATによってアドレス変換される。ローカルアドレスＬ１０４は、グローバルアドレスＧ１０４にStatic NATによってアドレス変換される。

【００８０】図１２においては、端末ドメインＡの欄にグローバルアドレスＧ１が付加され、サーバドメインＡの欄に２つのグローバルアドレスＧ３，Ｇ４が付加され、端末ドメインＢの欄にグローバルアドレスＧ１０１が付加され、サーバドメインＢの欄に２つのグローバルアドレスＧ１０３，Ｇ１０４が付加されている。

【００８１】図１３および図１４は、パケットフィルタリング情報生成部４６によって行なわれるパケットフィルタリング情報の作成手順を示すものである。以下、この作成手順の詳細を説明する。

【００８２】まず、図５に示すアクセス規則テーブルＴ２から１つのアクセス規則（例えば規則名ＰＪ１－１）を取り出す（ステップＳ２０１）。

【００８３】つぎに、取り出したアクセス規則からこのアクセス規則に属する適用ドメインfromを取り出し（ステップＳ２０２），この適用ドメインfromのドメイン名に対応する１～複数のホストアドレス（ローカルアドレス）を図４のドメイン定義テーブルＴ１から取り出す（ステップＳ２０３）。

【００８４】つぎに、先に取り出したアクセス規則に属する適用ドメインtoを取り出し（ステップＳ２０４）、この適用ドメインtoのドメイン名に対応する１～複数のホストアドレス（グローバルアドレス）を図１２のドメイン定義テーブルＴ１から取り出す（ステップＳ２０５）。

【００８５】つぎに、適用ドメインfromの１～複数のホストアドレス（ローカルアドレス）を発信元アドレス／ポート番号とし、適用ドメインtoの１～複数のホストアドレス（グローバルアドレス）を宛先アドレス／ポート番号とした全てのホストアドレスの組み合わせを何れかのファイアウォールのパケットフィルタリング情報としてパケットフィルタリング情報テーブルＴ４に登録する（ステップＳ２０６）。

【００８６】図５の規則名ＰＪ１－１の場合は、適用ドメインfrom（端末ドメインＡ）のホストアドレス（ローカルアドレス）がＬ１，Ｌ２で、適用ドメインto（サーバドメインＢ）のホストアドレス（グローバルアドレス）がＧ１０３、Ｇ１０４であるので、Ｌ１→Ｇ１０３、Ｌ１→Ｇ１０４、Ｌ２→Ｇ１０３，Ｌ２→Ｇ１０４の４つのパケットフィルタリング情報がファイアウォールＦＷ１用のものとして登録される。これら４つのパケットフィルタリング情報は、図１５の上側の４つの箱に示されている。

【００８７】つぎに、上記取り出したアクセス規則のプロトコル種別を図５に示すアクセス規則テーブルＴ２から取り出し、該取り出したプロトコル種別を上記登録したパケットフィルタリング情報にプロトコル種別として登録する（ステップＳ２０７）。

【００８８】さらに、登録したパケットフィルタリング情報に通信の方向（例えば双方向）と、通信の可否を追加登録する（ステップＳ２０８，２０９）。この追加登録は、所定のデータベースを用いて自動的に登録されるようにしてもよいし、パケットフィルタリング情報アドレス変換情報表示／編集部４２を介して管理者が追加登録するようにしてもよい。

【００８９】つぎに、前記取り出したアクセス規則からこのアクセス規則に属する適用ドメインtoを取り出し（図１４ステップＳ２１０）、この適用ドメインtoのドメイン名に対応する１～複数のホストアドレス（ローカルアドレス）を図４のドメイン定義テーブルＴ１から取り出す（ステップＳ２１１）。

【００９０】つぎに、前記取り出したアクセス規則に属する適用ドメインfromを取り出し（ステップＳ２１２）、この適用ドメインfromのドメイン名に対応する１～複数のホストアドレス（グローバルアドレス）を図１２のドメイン定義テーブルＴ１から取り出す（ステップＳ２１３）。

【００９１】つぎに、適用ドメインtoの１～複数のホストアドレス（ローカルアドレス）を発信元アドレス／ポート番号とし、適用ドメインfromの１～複数のホストアドレス（グローバルアドレス）を宛先アドレス／ポート番号とした全てのホストアドレスの組み合わせを何れかのファイアウォールのパケットフィルタリング情報としてパケットフィルタリング情報テーブルＴ４に登録する（ステップＳ２１４）。

【００９２】図５の規則名ＰＪ１－１の場合は、適用ドメインto（サーバドメインＢ）のホストアドレス（ローカルアドレス）がＬ１０３、Ｌ１０４で、適用ドメインfrom（端末ドメインＡ）のホストアドレス（グローバルアドレス）がＧ１であるので、Ｌ１０３→Ｇ１，Ｌ１０４→Ｇ１の２つのパケットフィルタリング情報がファイアウォールＦＷ２用のものとして登録される。これら２つのパケットフィルタリング情報は、図１６の下側の２つの箱に示されている。グローバルアドレスがＧ１の端末ドメインＡはBasic NATでポート番号をアドレス変換の対象にしていないので、パケットフィルタリング情報が２個になっている。

【００９３】つぎに、上記取り出したアクセス規則のプロトコル種別を図５に示すアクセス規則テーブルＴ２から取り出し、該取り出したプロトコル種別を上記登録したパケットフィルタリング情報にプロトコル種別として登録する（ステップＳ２１５）。さらに、登録したパケットフィルタリング情報に通信の方向（例えば双方向）と、通信の可否を追加登録する（ステップＳ２１６，２１７）。

【００９４】ステップＳ２２０においては、図５に示すアクセス規則テーブルＴ２につぎのアクセス規則があるか否かが判定される。次のアクセス規則がある場合は、このアクセス規則に関して前記と同様の手順が行われることにより、読み出したアクセス規則に対応するパケットフィルタリング情報が作成され、作成されたパケットフィルタリング情報は前記同様にしてパケットフィルタリング情報テーブルＴ４に記憶される。

【００９５】図５のアクセス規則テーブルＴ２に登録された全てのアクセス規則について、前述した処理を繰り返すことにより、図１５および図１６に示すような、各ＬＡＮ１２，１３のファイアウォールＦＷ１，ＦＷ２のパケットフィルタリング情報が作成される。

【００９６】図５の規則名ＰＪ１－２の場合は、適用ドメインfrom（端末ドメインＢ）のホストアドレス（ローカルアドレス）がＬ１０１、Ｌ１０２で、適用ドメインto（サーバドメインＡ）のホストアドレス（グローバルアドレス）がＧ３，Ｇ４であるので、Ｌ１０１→Ｇ３，Ｌ１→Ｇ４，Ｌ１０２→Ｇ３，Ｌ１０２→Ｇ４の４つのパケットフィルタリング情報がファイアウォールＦＷ２用のものとして登録される。これら４つのパケットフィルタリング情報は、図１６の上側の４つの箱に示されている。

【００９７】さらに、図５の規則名ＰＪ１－２の場合

は、適用ドメインto（サーバドメインA）のホストアドレス（ローカルアドレス）がＬ３，Ｌ４で、適用ドメインfrom（端末ドメインB）のホストアドレス（グローバルアドレス）がＧ１０１であるので、Ｌ３→Ｇ１０１／＊，Ｌ３→Ｇ１０１／＊，Ｌ４→Ｇ１０１／＊，Ｌ４→Ｇ１０１／＊の４つのパケットフィルタリング情報がファイアウォールＦＷ１用のものとして登録される。これら２つのパケットフィルタリング情報は、図１５の下側の２つの網に示されている。グローバルアドレスがＧ１０１の端末ドメインBはNAPTでポート番号をアドレス変換の対象にしているので、パケットフィルタリング情報が４個になっている。

【００９８】このようにこの実施の形態においては、各ＬＡＮ１２，１３の運用ポリシーとしてのドメイン定義テーブルＴ１、アクセス規則テーブルＴ２と、空グローバルアドレステーブルＴ５と、ＮＡＴ設定規則テーブルＴ６と、サービス定義テーブルＴ７とに基づいて各ＬＡＮ１２，１３のファイアウォールＦＷ１、ＦＷ２で用いてＮＡＴアドレス変換情報Ｄ１ｂ，Ｄ２ｂおよびパケットフィルタリング情報Ｄ１ａ，Ｄ２ａを生成するようにしたので、ＮＡＴを用いて複数のＬＡＮ間をインターネット接続するための各ファイアウォールでの所要の設定情報を一括して簡単に作成することができる。また、人間に判りやすい運用ポリシー定義を用いたので、専門知識も持たない者でもファイアウォールの設定情報を簡単に作成することができる。

【００９９】なお、上記実施の形態においては、ネットワーク管理装置は、インターネットを介して接続される２つのＬＡＮを管理対象としたが、インターネットを介して接続される３つ以上のＬＡＮを管理対象にしてもよい。また、上記実施の形態においては、各ＬＡＮには、１つの端末ドメインおよび１つのサーバドメインが含まれるようにしたが、前述したように、１つのＬＡＮに複数の端末ドメインおよび複数のサーバドメインが含まれるような網構成にも本発明は適用可能である。

【０１００】

【発明の効果】以上説明したように、この発明によれば、複数のＬＡＮの運用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレス、ＮＡＴ設定規則、サービス定義に関する情報を用いてＮＡＴアドレス変換情報およびパケットフィルタリング情報を生成するようにしたので、ＮＡＴを用いて複数のＬＡＮ間をインターネット接続するための各ファイアウォールでの所要の設定情報を一括して簡単に自動作成することができるようになる。

【０１０１】つぎの発明によれば、端末とサーバとを別グループとして複数のグループに分け、該分けたグループ間でのアクセス規則を前記運用ポリシーとして前記データベースに蓄積しているので、人間に判りやすい運用ポリシー定義を用いることができ、専門知識も持たない者でもファイアウォールの設定情報を簡単に作成することができる。

【０１０２】つぎの発明によれば、当該ＬＡＮの１つの端末グループから他のＬＡＮの１つのサーバグループへのアクセスを単位として、管理すべき複数のＬＡＮ内に含まれる全ての端末グループおよびサーバグループについてのアクセス規則を登録するようにしているので、人間に判りやすい運用ポリシー定義を用いることができ、専門知識も持たない者でもファイアウォールの設定情報を簡単に作成することができる。

【０１０３】つぎの発明によれば、アクセス規則にグローバルアドレスの割当数がグループ毎に設定しているので、専門知識も持たない者でもファイアウォールの設定情報を簡単かつ正確に作成することができる。

【０１０４】つぎの発明によれば、アクセス規則に、プロトコル種別、サービス種別、同じグループ内での各端末の同時接続の有無が登録しているので、専門知識も持たない者でもファイアウォールの設定情報を簡単かつ正確に作成することができる。

【０１０５】つぎの発明によれば、端末およびサーバの区別、自グループ内の端末またはサーバの同時接続の有無、サービス指定ポート番号の有無などの登録情報に基づいてＮＡＴ種別が分類されるので、専門知識も持たない者でもＮＡＴ種別を簡単に分類することが可能になる。

【０１０６】つぎの発明によれば、サービス定義には、サービス種別、端末およびサーバの区別、指定ポート番号が登録されているので、専門知識を持たない者でもサービス定義を正確に登録することができる。

【０１０７】つぎの発明によれば、運用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレス、ＮＡＴ設定規則、サービス定義に関する情報を編集し、該編集結果を前記データベースに登録する手段を備えているので、運用ポリシー、ＬＡＮの構成などが変更された場合にもこれに容易に対処することができる。

【０１０８】つぎの方法発明によれば、複数のＬＡＮの運用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレス、ＮＡＴ設定規則、サービス定義に関する情報を用いてＮＡＴアドレス変換情報およびパケットフィルタリング情報を生成するようにしたので、ＮＡＴを用いて複数のＬＡＮ間を接続するための各ファイアウォールでの所要の設定情報を一括して簡単に作成することができる。

【図面の簡単な説明】

【図１】　この発明を適用するインターネット接続の網構成の一例を示すブロック図である。

【図２】　この発明にかかるファイアウォール管理装置に内蔵される管理ソフトウェアの機能構成の一例を示したブロック図である。

【図３】　ファイアウォール接続ドメインテーブルの登録内容を例示する図である。

【図４】　ドメイン定義テーブルの登録内容を例示する図である。

【図５】　アクセス規則テーブルの登録内容を例示する図である。

【図６】　変グローバルアドレステーブルの登録内容を例示する図である。

【図７】　ＮＡＴ設定規則テーブルの登録内容を例示する図である。

【図８】　サービス定義情報テーブルの登録内容を例示する図である。

【図９】　アドレス変換情報生成部で行われるアドレス変換情報作成処理の手順を示すフローチャートである。

【図１０】　作成された一方のファイアウォールのアドレス変換情報を示す図である。

【図１１】　作成された他方のファイアウォールのアドレス変換情報を示す図である。

【図１２】　アドレス変換情報作成後のドメイン定義テーブルの登録内容を示す図である。

【図１３】　パケットフィルタリング情報生成部で行われるパケットフィルタリング情報作成処理の手順（その一）を示すフローチャートである。

【図１４】　パケットフィルタリング情報生成部で行われるパケットフィルタリング情報作成処理の手順（その二）を示すフローチャートである。

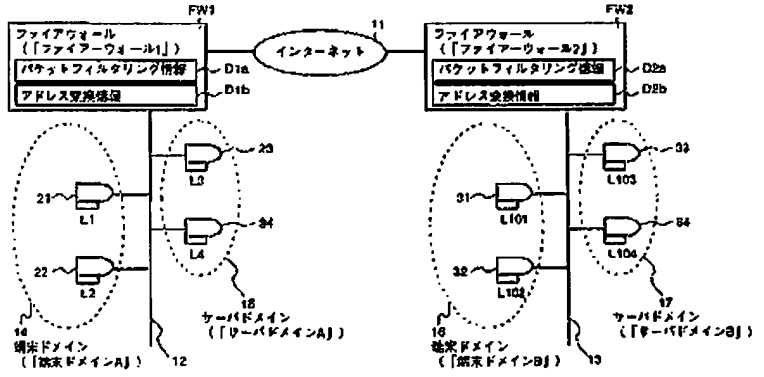
＊【図１５】　作成された一方のファイアウォールのパケットフィルタリング情報を示す図である。

【図１６】　作成された他方のファイアウォールのパケットフィルタリング情報を示す図である。

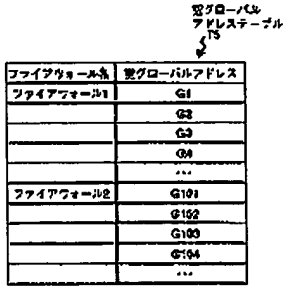
【符号の説明】

１１　インターネット、　１４　端末ドメイン、　１５　サーバドメイン、１６　端末ドメイン、　１７　サーバドメイン、　２１　端末、　２３　サーバ、　２４　サーバ、　３１　端末、　３３　サーバ、　３４　サーバ、　４０管理ソフトウェア、　４１　ドメイン定義アクセス規則入力部、　４２　パケットフィルタリング情報アドレス変換情報表示／編集部、　４３　変グローバルアドレステーブル表示／編集部、　４４　ＮＡＴ設定規則サービス定義編集部、４５　アドレス変換情報生成部、　４６　パケットフィルタリング情報生成部、　４７　ファイアウォール接続ドメイン入力部、　Ｄ１ａ　パケットフィルタリング情報、　Ｄ２ａ　パケットフィルタリング情報、　Ｄ１ｂ　アドレス変換情報、　Ｄ２ｂ　アドレス変換情報、　ＦＷ１　ファイアウォール、　ＦＷ２　ファイアウォール、　Ｔ１　ドメイン定義テーブル、Ｔ２　アクセス規則テーブル、　Ｔ３　アドレス変換情報テーブル、　Ｔ４　パケットフィルタリング情報テーブル、　Ｔ５　変グローバルアドレステーブル、　Ｔ６　ＮＡＴ設定規則テーブル、　Ｔ７　サービス定義テーブル、　Ｔ８　ファイアウォール接続ドメインテーブル。

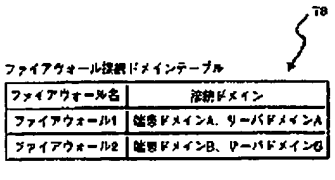
【図１】



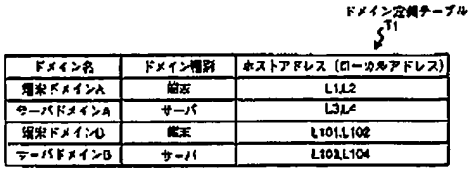
【図６】



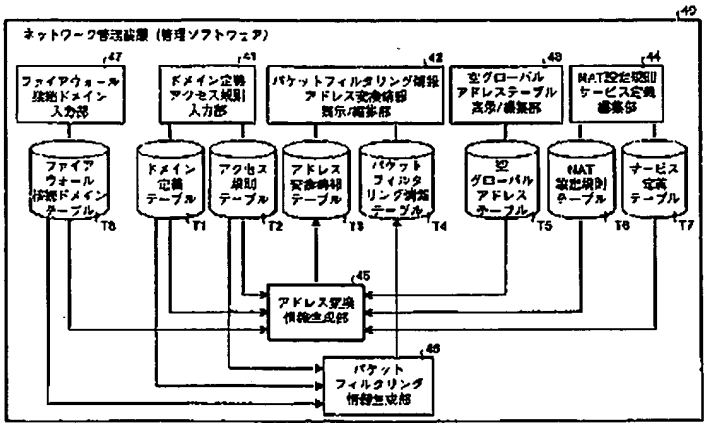
【図３】



【図４】



【図2】



【図5】

【図7】

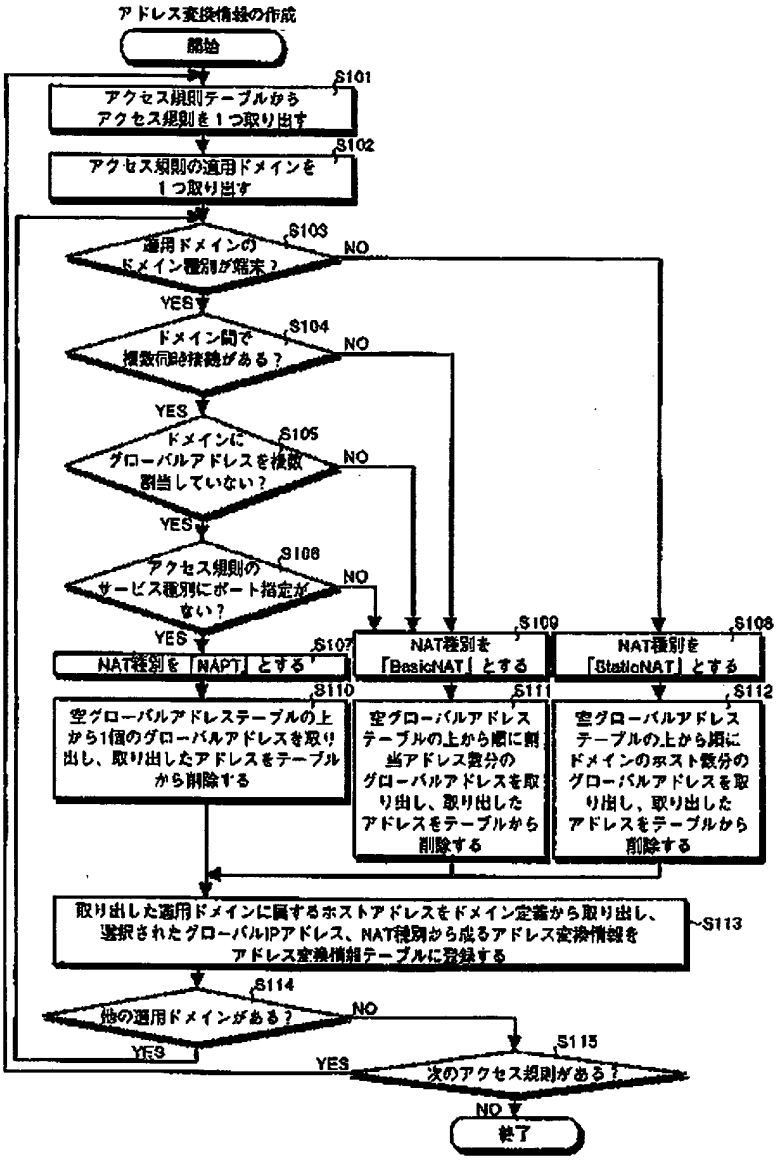
【図8】

【図10】

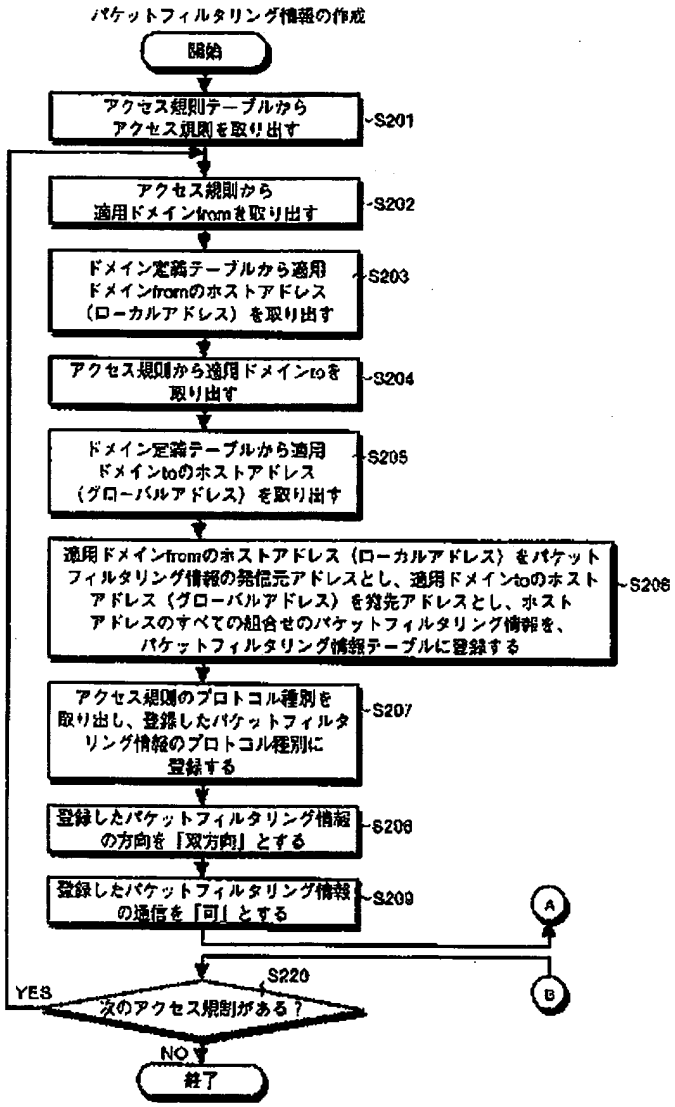
【図11】

【図12】

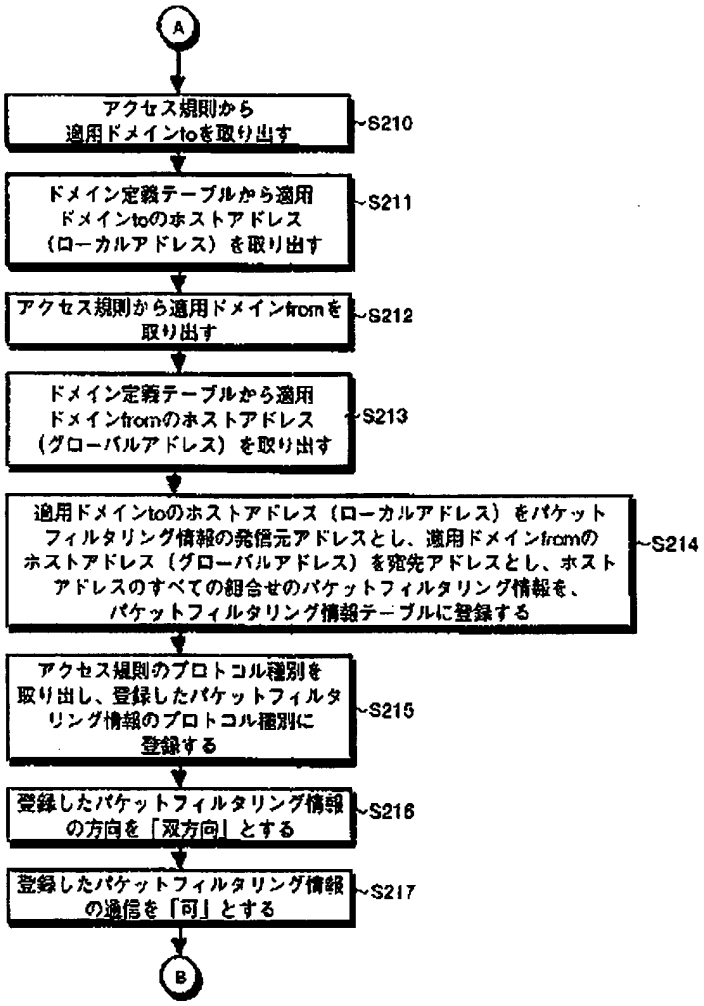
【図9】


アドレス変換情報の作成
開始
S101
アクセス規則テーブルから
アクセス規則を1つ取り出す
S102
アクセス規則の適用ドメインを
1つ取り出す
S103
適用ドメインの
ドメイン種別が端末？
NO
YES
S104
ドメイン間で
複数同時接続がある？
NO
YES
S105
ドメインに
グローバルアドレスを複数
割当していない？
NO
YES
S106
アクセス規則の
サービス種別にポート指定が
ない？
NO
YES
S107
NAT種別を「NAPT」とする
S109
NAT種別を
「BasicNAT」とする
S108
NAT種別を
「StaticNAT」とする
S110
空グローバルアドレステーブルの上
から1個のグローバルアドレスを取り
出し、取り出したアドレスをテーブル
から削除する
S111
空グローバルアドレス
テーブルの上から順に割
当アドレス数分の
グローバルアドレスを取
り出し、取り出した
アドレスをテーブルから
削除する
S112
空グローバルアドレス
テーブルの上から順に
ドメインのホスト数分の
グローバルアドレスを取
り出し、取り出した
アドレスをテーブルから
削除する
S113
取り出した適用ドメインに属するホストアドレスをドメイン定義から取り出し、
選択されたグローバルIPアドレス、NAT種別から成るアドレス変換情報を
アドレス変換情報テーブルに登録する
S114
他の適用ドメインがある？
NO
YES
S115
次のアクセス規則がある？
YES
NO
終了

【図１３】


パケットフィルタリング情報の作成
開始
アクセス規則テーブルから
アクセス規則を取り出す
S201
アクセス規則から
適用ドメインfromを取り出す
S202
ドメイン定義テーブルから適用
ドメインfromのホストアドレス
（ローカルアドレス）を取り出す
S203
アクセス規則から適用ドメインtoを
取り出す
S204
ドメイン定義テーブルから適用
ドメインtoのホストアドレス
（グローバルアドレス）を取り出す
S205
適用ドメインfromのホストアドレス（ローカルアドレス）をパケット
フィルタリング情報の発信元アドレスとし、適用ドメインtoのホスト
アドレス（グローバルアドレス）を宛先アドレスとし、ホスト
アドレスのすべての組合せのパケットフィルタリング情報を、
パケットフィルタリング情報テーブルに登録する
S206
アクセス規則のプロトコル種別を
取り出し、登録したパケットフィルタ
リング情報のプロトコル種別に
登録する
S207
登録したパケットフィルタリング情報
の方向を「双方向」とする
S208
登録したパケットフィルタリング情報
の通信を「可」とする
S209
A
B
S220
YES
次のアクセス規則がある？
NO
終了

【図１４】



【図１５】

ファイアウォールFW1

パケットフィルタリング情報 D1a

発信元アドレス/ポート番号	宛先アドレス/ポート番号	プロトコル種別	方向	通信
L1/*	G102/*	TCP	双方向	可
L1/*	G104/*	TCP	双方向	可
L2/*	G103/*	TCP	双方向	可
L2/*	G104/*	TCP	双方向	可
L3/*	G101/*	TCP	双方向	可
L3/*	G101/*	TCP	双方向	可
L4/*	G101/*	TCP	双方向	可
L4/*	G101/*	TCP	双方向	可

【図１６】

ファイアウォールFW2

パケットフィルタリング情報 D2a

発信元アドレス/ポート番号	宛先アドレス/ポート番号	プロトコル種別	方向	通信
L101/*	G3/*	TCP	双方向	可
L101/*	G4/*	TCP	双方向	可
L102/*	G3/*	TCP	双方向	可
L102/*	G4/*	TCP	双方向	可
L103/*	G1/*	TCP	双方向	可
L104/*	G1/*	TCP	双方向	可